



04/05/2020

Boot LoaderProject

Phase 2 Final Report

Submitted to Dr. Karim Sobh

Submitted by:

Menna Elzahar 900182968

Omar Elsayed 900183884

Youssef Hussien 900183162

Nourhan Moussa 900172701

Tasks Done

In this phase, we have

1. disabled **PIC**
2. loaded **IDT descriptor**
3. wrote the **video_cl_16** function to clear the screen to switch to long mode
4. switched to **long mode**
5. built **page table** through page walk mechanism while keeping a **bit map** for the physical addresses of type 1
6. wrote a **tester** function to test out page table

Assumptions and Findings

Here is a pseudocode of how we have built our page table to map our physical memory.

Initialize starting physical address for page table levels allocation by 0x100000 in rcx.

Initialize starting physical address to be mapped in level 4 by 0x0 in rbx.

Loop over memory regions and set type 1 to 0 and any other type to 1.

Create bit map at effective address 0x500000.

for (i=0 ; i<memory_size generated from memscanner function; i+=4KB) call page_walk(i);

page_walk (virtual address){

1. extract offset in r9, 4 9-bit indices in r10, r11, r12, and r13 respectively where r13 has the MS 9 bits.
2. Use r13 to reach entry needed in PML4 (multiply r13 by 8 and add to it the beginning address of this page).
3. Check entry content
 - a. If it's null, jump to allocate
 - i. In allocate, we loop over memory regions to check if our last_physical_address (in rax) is of type 1
 - ii. If not increment rax by 4KB and keep looping until an address of type 1 is found
 - iii. Jump to approve_allocate
 - iv. Reserve 512 entries by initializing their content to zero starting from physical address found in step ii.
 - v. Put last physical address in the current page entry then increment it by 4KB and update CR3. The jump to label skip
 - b. Else skip
 - i. Repeat the same steps (step 2 and 3) entries indicated by next 9 bits. Do the same until level 4 is allocated.

In level 4, search in the bitmap for a valid physical address and assign it to the entry indicated by r10 (least 9 bits before offset). Then, set the corresponding bit in bitmap to 1.

}

ScreenShots



